



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/067,319	02/07/2002	Swati Deshmukh	19903.0016	7037

23517 7590 12/23/2005

SWIDLER BERLIN LLP
3000 K STREET, NW
BOX IP
WASHINGTON, DC 20007

EXAMINER

NGUYEN, QUANG N

ART UNIT

PAPER NUMBER

2141

DATE MAILED: 12/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/067,319

Applicant(s)

DESHMUKH ET AL.

Examiner

Quang N. Nguyen

Art Unit

2141

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 10 November 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,16,17,32,33 and 48-81 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,16,17,32,33 and 48-81 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Detailed Action

1. This Office Action is in response to the Amendment filed on 11/10/2005. Claims 1, 16-17, 32-33 and 48 have been amended. Claims 2-15, 18-31 and 34-47 have been cancelled. Claims 49-81 have been added as new claims. Claims 1, 16-17, 32-33 and 48-81 are presented for examination.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. **Claims 1, 16-17, 32-33 and 48-81 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ackroyd (US 2003/0131256 A1), hereinafter "Ackroyd", in view of Hansen et al. (US 6,493,755), hereinafter "Hansen".**

4. As to claim 1, Ackroyd teaches a method of reporting malware events, comprising the steps of:

detecting a malware event with one of a plurality of levels using a malware scanner, the malware event comprising **at least one of**: completion of a malware scan,

a process failure relating to malware scanning, a missing log file, detection of malware, or failure of a response to malware (*detection of malware items by the malware scanners operating*) (Ackroyd, paragraph [0025]);

determining a level of the detected malware event (*identifying patterns of malware detection*) (Ackroyd, paragraphs [0027-0029]);

comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels (*at step 48, a determination is made as to whether or not any of the thresholds has been exceeded or any of the patterns matched*) (Ackroyd, paragraphs [0027-0029]); and

transmitting a notification of the detected malware event, based on the comparison of the level of the detected malware event to the event trigger threshold (*if thresholds have been exceeded or patterns matched, then one or more predefined anti-malware actions are triggered and will be directed to the appropriate problem area within the network concerned*) (Ackroyd, paragraphs [0027-0029]);

wherein the level of the malware event (or the level of the event trigger threshold) comprises one of: information malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected (*for example, a particular preferred anti-malware action maybe triggered is to force an update of malware definition data being used; to deal with the malware by disinfecting, repairing*

or deleting the infected files or emails as appropriate and possibly isolating one or more portions of the computer network from the rest of the computer network in order to isolate a malware outbreak) (Ackroyd, paragraphs [0011-0014 and 0030-0032]).

However, Ackroyd does not explicitly teaches transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold; wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time.

In an analogous art, Hansen teaches the computer network management and automatically defining conditions under which a user/administrator is notified of network activity, wherein notification rules would include notification actions specified by the administrator, including executing a script at the server location, reporting the particular event occurrence on a separate event log saved in the network management software, *(i.e., these notification actions could be implemented in real-time and/or eventually)* indicating a change in the state of the device by creating a sound on the host computer, sending an email to a remote address, and sending a page to the administrator's pager *(i.e., these notification actions usually being implemented in real-time)* when a pre-selected network event occurs. In addition, a corresponding alarm severity class/level can be set to limit triggering of the notification rule based on the extend to which the threshold has been exceeded, for example, cleared (or informational), indeterminate, minor, major and critical alarm classes/levels. Specially, the administrator is able to

configure the notification function provided by the management software to limit notification, or device status reporting (*i.e., configurable to control an amount of the notifications*), to only those instances in which a particular predefined network event occurs (Hansen, C1:L40 – C2:L44 and C4: L20-38).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Ackroyd and Hansen to include transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold; wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time since such methods were conventionally employed in the art to allow the system to detect and handle malware in a networked environment and to reduce network traffic by limiting notification, or device status reporting to only those instances in which certain pre-selected network events occur (Hansen, C4: L20-38).

5. As to claim 16, Ackroyd-Hansen teaches the method of claim 1, further comprising the step of transmitting an alert to an administrator indicating occurrence of the detected malware in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold (*i.e., creating a sound on the host computer, sending an email to a remote address, and sending a page to the administrator's pager when a certain pre-selected network event occurs*) (Hansen, C2: L31-44).

6. As to claims 49-50, Ackroyd-Hansen teaches the method of claim 1, wherein the event trigger threshold is set at a management server by setting policies in the malware management program (*the administrator 12 is able to request the network management software 14 to execute a notification action only when a pre-selected event occurs*) (Hansen, C4: L20-38).

7. As to claim 51, Ackroyd-Hansen teaches the method of claim 1, wherein the event trigger threshold is distributed to a plurality of malware agents residing in a plurality of user systems (*malware scanners operating on client computers*).

8. As to claims 52-53, Ackroyd-Hansen teaches the method of claim 1, wherein if the level of the detected malware event is less than the event trigger threshold, the notification of the event is not transmitted until an eventual periodic event transmission or until a request by a management server is received (*the system waits for predetermined regular times to occur at which the policy organizing server 32 issues appropriate queries to the database to generate the predetermined reports which are then compared with predetermined patterns and network-wide threshold to trigger predefined anti-malware actions*) (Ackroyd, paragraphs [0027-0029]).

9. As to claims 54-59, Ackroyd-Hansen teaches the method of claim 1, wherein the level of the event trigger threshold is selected from a ranked set of levels including, from least critical to most critical with progressively greater levels, as follows cleared (or

informational), indeterminate, minor, major and critical (*as alarm severity classes/levels*) (Hansen, C1:L49 – C2:L2).

10. Claims 17, 32 and 60-70 are corresponding system claims of method claims 1, 16 and 49-59; therefore, they are rejected under the same rationale.

11. Claims 33, 48 and 71-81 are corresponding computer program product claims of method claims 1, 16 and 49-59; therefore, they are rejected under the same rationale.

12. Applicant's arguments as well as request for reconsideration filed on 11/10/2005 have been fully considered but they are moot in view of the new ground(s) of rejection.

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


Art Unit: 2141

14. Further references of interest are cited on Form PTO-892, which is an attachment to this office action.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Quang N. Nguyen whose telephone number is (571) 272-3886.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's SPE, Rupal Dharia, can be reached at (571) 272-3880. The fax phone number for the organization is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


RUPAL DHARIA
SUPERVISORY PATENT EXAMINER